U-14,150/RSE-4 [redacted] 26 April 1984

FILE DESIGNATION STAT

CONCURRENCES

MEMORANDUM FOR THE DEPUTY UNDER SECRETARY OF DEFENSE FOR POLICY

SUBJECT: DoD Trusted Computer System Evaluation Criteria

1. Reference is made to SD Form 106, dated 15 December 1983, (enclosure 1) which forwarded the DoD Trusted Computer Systems Evaluation Criteria to DIA for review and comment. DIA has reviewed the document and strongly supports the need for and concept of standard criteria against which system security strengths and weaknesses can be measured. NSA and the other organizations that developed this document should be commended for their professional efforts and contribution to the DoD Computer Security Program. However, the DIA review concluded that the criteria, when considered as a proposed DoD standard, do not meet the requirements of the DoD Intelligence Community; therefore, the Agency does not concur in this document as written.

2. There are two areas of shortfall in the document that require modification. First, the document does not provide a clear and accurate correlation between security policies of Director of Central Intelligence (DCI) and DoD for Sensitive Compartmented Information (SCI) and the security levels established by the document. Second, the document allows a user to exceed previously defined privileges permitted by DCI and DoD security policy. Additionally, provision should be made for periodic revision of the criteria to maintain concurrency with changing security policy and technology.

3. DIA believes that although improvements in computer security must be afforded high priority, we must also ensure that computer security standards are developed which consider the operational requirements for dissemination of all-source intelligence to users at every echelon of military command. Accordingly, the Agency considers that tailoring of security criteria is necessary to satisfy individual operational requirements and provide cost effective retrofitting to existing systems. Developing new computer security techniques and retrofitting them to existing systems have been shown to be extremely costly. Thus, DIA recommends that the implementation of the standard proceed at a measured pace and provide for current operational and systems already under development to be exempted, if necessary, from portions of the criteria.

4. DIA has prepared substantive modifications to the document and provided them in enclosure 2. These changes address our concerns and their incorporation into the document is essential. DIA staff assistance is available to facilitate the inclusion of these changes in the document. After the DoD staffing process is completed, DIA requests that the document be returned to the Agency for final review.

2 Enclosures a/s
COORDINATION CY
RSE R/F CY
RSD R/F CY
RS-A R/F CY
RSE-4 R/F CY
DR CY

RETURN FOR FILING TO

DoD DIRECTIVES SYSTEM COORDINATION AND CONTROL RECORD

ILLEGIB

b. TYPED NAME *(Last, first, M.I.)* Stilwell, Richard G., GEN. USA(Ret.)	Epperly, Eugene V.		
c. TITLE Deputy Under Secretary of Defense(Policy)	c. OFFICE SYMBOL CSP,ODUSD(P)	d. EXTENSION 55179	e. ROOM NUMBER 3C283
		7. DATE FORWARDED *(YYMMDD)* 15 DEC 1983	8. RETURN DATE 15 APR 1984

6. REMARKS

This action formally coordinates the attached as a standard for use in meeting system security evaluation and approval responsibilities assigned by DoDD 5200.28. It represents the culmination of over 10 years of DoD effort - relevant background is appended for additional information.

Proposed guidance for specific application of the criteria to current policy and system security modes set forth in DoDD 5200.28 and DoD 5200.28-M will be separately developed and coordinated.

Request recommended changes be submitted with rationales in "line-in/line-out" format.

FOR USE OF ORIGINATING OFFICE ONLY *(Check appropriate box(es) below)*

THE CLASSIFICATION IS: *(See DoD Regulation 5200.1-R)*

□ TOP SECRET
□ SECRET
□ CONFIDENTIAL
☒ UNCLASSIFIED
□ OTHER *(Specify)*

THE DOCUMENT WILL BE PUBLISHED AS A RULEMAKING DOCUMENT IN THE FR. *(See DoD Directive 5400.9)*

□ YES ☒ NO

9. TO ADDRESSEES LISTED BELOW: The attached draft is forwarded for review and comment.

a. If the draft as written is approved, please indicate concurrence by signing and dating the appropriate space below. (Signature level must comply with paragraphs D.2.b. through D.2.d., Chapter 2, DoD 5025.1-M.)

b. If changes are recommended please attach a separate memorandum covering the recommendations and so indicate in the appropriate space below.

X	UNDER SEC DEF FOR POLICY	X	SECY OF THE ARMY
X	UNDER SEC DEF FOR RESEARCH AND ENGINEERING	X	SECY OF THE NAVY
X	ASST. SEC DEF *(Comptroller)*	X	SECY OF THE AIR FORCE
	ASST. SEC DEF *(Health Affairs)*	X	CHAIRMAN, JOINT CHIEFS OF STAFF
X	ASST. SEC DEF *(International Security Affairs)*	X	DIR, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
X	ASST. SEC DEF *(International Security Policy)*	X	DIR, DEFENSE AUDIOVISUAL AGENCY
X	ASST. SEC DEF *(Legislative Affairs)*	X	DIR, DEFENSE COMMUNICATIONS AGENCY
X	ASST. SEC DEF *(Manpower, Reserve Affairs, and Logistics)*	X	DIR, DEFENSE CONTRACT AUDIT AGENCY
X	ASST. SEC DEF *(Public Affairs)*	X	DIR, DEFENSE INTELLIGENCE AGENCY See memo and comments.
X	GENERAL COUNSEL, DoD	X	DIR, DEFENSE INVESTIGATIVE SERVICE
X	INSPECTOR GENERAL, DoD	X	DIR, DEFENSE LOGISTICS AGENCY
	ASST. TO THE SEC DEF *(Atomic Energy)*	X	DIR, DEFENSE MAPPING AGENCY
	ASST. TO THE SEC DEF *(Intelligence Oversight)*	X	DIR, DEFENSE NUCLEAR AGENCY
	DIRECTOR, PROGRAM ANALYSIS & EVALUATION	X	DIR, DEFENSE SECURITY ASSISTANCE AGENCY
		X	DIR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE

PREVIOUS EDITIONS ARE OBSOLETE.

DIA COMMENTS ON

DoD Trusted Computer System Evaluation Criteria

General

A mechanism for change for this Standard must be established which provides for a DoD review of the document in order to insure concurrency is maintained with the rapidly evolving security policy and technology.

In the Criteria, the term "trusted" is used for all criteria from C1 through A1. C1 systems are certainly not "trustworthy". Suggest using different terms for different levels of security confidence which are independent of the type of data or information contained in the system. Suggest that the terms "trusted", "secure", and "private" be used to describe the security confidence levels offered by a Division A, B, and C system respectively.

Specific

page 12, Section 2.1.1.1, Discretionary Access Control

Change: Replace the sentence "The enforcement mechanism . . . shall allow users to specify and control sharing of those objects by named individuals . . . ."
with: "The enforcement mechanism . . . shall allow users to specify and control sharing of those objects, initially generated by the user, by named individuals . . . ."

page 12, Section 2.1.1.2, Object Reuse

Change: Add new section
"2.1.1.2 Object Reuse
The TCB shall be capable of clearing, or overwriting any storage object."

Rationale:
To reflect DCI policy on object reuse.

page 15, Section 2.2.1.1, Discretionary Access Control

First Incorporate the change made in 2.1.1.1 and Second:

Change: Replace the last sentence of the paragraph: "Access permission to an object by users not already possessing access permission shall only be assigned by authorized users."
with: "Access permission to an object by users not already possessing access permission shall only be assigned by the user who initially generated the object and is still responsible and authorized to grant access or by the Data Base Administrator or System Security Officer for all other objects in the system."

Propagate the changes made in Section 2.1.1.1 and 2.2.1.1 into:

page 20, Section 3.1.1.1
page 26, Section 3.2.1.1
page 33, Section 3.3.1.1
page 43, Section 4.1.1.1

Rationale for the above two changes:
A user should only be capable of expanding access to objects which belong to the particular user, not for objects to which that user only has access. Otherwise any user could usurp the authority of the Data Base Administrator or System Security Officer.

page 17.1

Change: Insert new Class: 2.3 Class (C3): Labeled Object Protection

Class (C3) systems require all of the features of Class (C2). In addition, the capability must exist for accurate labeling of data to at least the granularity of a file and for labeling of exported information. The capability to audit changes in data labels must be present. Configuration management controls are required to manage source and object code changes. Device labels (for at least remote terminals) shall be present.

FULL TEXT OF CHANGE CAN BE FOUND AT ANNEX 1.

Rationale:
DCID minimum requirements for System High mode of operation differ from and are not compatible with class C2 nor B1 but rather fall between them, the requirements are:

- Remote terminal authentication
- Security classification and handling caveats identified with information in the system
- Labeling of output
- Audit trails
- Configuration Management Controls

page 20, Section 3.1, Class (B1): Labeled Security Protection, first paragraph

Change: Replace first three sentences
with: Class (B1) systems require all the features for class (C3). In addition, an informal statement of the security policy model, and mandatory access control over named subjects and objects must be present.

Rationale:
The reference to labeling has been removed as it is covered in the new Class (C3).

page 24, Section 3.1.3.1.3, Formal Analysis

Change: add new section
"3.1.3.1.3, Formal Analysis
Formal methods shall be used to investigate and document the behavior of the TCB under anomalous environmental conditions such as hardware failure."

Propagate the changes made in Section 3.1.3.1.3 into:
new section # 3.2.3.1.5
new section # 3.3.3.1.6
new section # 4.1.3.1.6

Rationale: Formal Design Verification Methods assume that the system being verified is closed and unaffected by environmental conditions. This is a reasonable assumption to make in verifying a design, but it should be extended with the notion that the real system will be open to influence from the environment. Formal methods can be used to investigate the behavior of a design under environmental influence (to a point). This additional step in use of formal verification technology should be incorporated into the criteria.

An instance of the specific use of such a methodology is due to L. J. La Padula, to be documented in part II, Vol. 4 of MTR 8756, DODIIS Security Protection for Information Exchange: Formal Design Verification of DNSIX.

page 24, Section 3.1.3.1.4, Integrity/Deadlock Analysis

Change: add new section
"3.1.3.1.4, Integrity/Deadlock Analysis
Evidence shall be provided that deadlocks cannot occur or that they can be securely resolved by the TCB when they occur. Deadlock resolution algorithms shall be subjected to detailed analysis to provide such evidence. Evidence shall be provided that no critical datum is shared within the system that is controlled by the TCB. Scheduler algorithms and critical (unshareable) data allocation shall be subjected to detailed analysis to provide such evidence."

Propagate the changes made in Section 3.1.3.1.4 into:
new section # 3.2.3.1.6
new section # 3.3.3.1.7
new section # 4.1.3.1.7

Rationale:
It has been shown that a system which employs an unrestricted, non-trivial scheduler has either a deadlock problem or a data integrity problem or both. The TCB would seem to employ such a scheduler as the mandatory security policy calls for dynamic realignment of resource allocations in consonance with changes in subject security level.

See 'Harmonious Cooperation of Processes Operating on a Common Set of Data,' parts 1,2, and 3, MTR-2254, 1972, D. E. Bell and L. J. La Padula

page 24, Section 3.1.3.1.5, Network Integrity/Stability

Change: add new section
"3.1.3.1.5, Network Integrity/Stability
An analysis shall be performed to show that the security provided by interacting TCBs is stable under the full range of normal networking operations, and the full range of possible TCB architectural combinations."

Propagate the changes made in Section 3.1.3.1.5 into:
new section # 3.2.3.1.7

new section # 3.3.3.1.8
new section # 4.1.3.1.8

Rationale:
If an interaction is unstable, then it is difficult to see how it could be considered secure. Since interactions among non-symmetric TCBs will take place (such as the interconnection of a B2 and a C2 system), it is not clear that stability will be achieved. Therefore, it is not clear that security will be maintained.

page 30, Section 3,2,3,1,3, Covert Channel Analysis

Change: delete section

Rationale:
The perceived threat which this is supposed to protect against is not supported in operational experience. The references used to support the section titled "A Guideline on Covert Channels", page 79, are open literature sources and thus do not document an actual threat.

As described on page 79, protecting against covert channels are expensive in system resources. This expense for an undocumented threat is excessive for the B2 level of system protection and should be eliminated.

page 31, Section 3.2.3.2.2, Design Specification and Verification

Change: Replace phrase at beginning of first sentence "A formal model of the security policy . . . ."
with: the same phrase from the B1 class to read "An informal or formal model of the security policy . . . ."

Rationale:
An inconsistancy exists between requiring the formal model and permitting a Descriptive Top Level Specification (DTLS).

page 64, Section 6.2, A Formal Security Policy Model, third line from bottom of page.

Change: Replace ". . . relation between the clearance of the subject and the . . ."
with: " . . . relation between the clearance of the subject (modified to be expressed as the session security level) and the . . ."

Rationale:
Mandatory security enforcement should be based on the session security level not upon the subject (i.e. current user) security level. This protects against compromise when entities between the user and the object are not protected to levels as high as the user's security level. It also provides the opportunity for intelligence analysts on systems offering mandatory protection to voluntarily lower their session security level in order to extract information at lower than their user maximum classifiation level.

pages 69-77, Section 7.0, The Relationship Between Policy and the Criteria

Change: Reference Defense Intelligence Agency Manual (DIAM) 50-4, "Security of Compartmented Computer Operations (U)," 24 June 1980 (CONFIDENTIAL)

Rationale:
DIAM 50-4 specifies the national level policy for foreign intelligence and Sensitive Compartmented Information (SCI) for DoD.

page 79, Section 8.0, A Guideline on Covert Channels, Third paragraph, first sentence

Change: Replace ". . . one hundred (100) bits per second . . ."
with: ". . . one thousand (1,000) bits per second . . ."

Rationale:
The threshold for covert channel analysis of 100 BPS is too low. A higher threshold is more economically realistic.

page 81, Section 9.0, A Guideline on Configuring Mandatory Access Control Features

Change: Replace the sentence "* The number of non-hierarchial categories should be greater than or equal to twenty-nine (29)."
with: "* The number of non-hierarchial categories should be greater than or equal to sixty four (64) and incrementable in integer multiples of 64."

Rationale:
When DIA originally provided the estimate of 29 it was understood to apply only to SCI compartments. Since the time of that estimate, the value has been expanded to include categories other than SCI compartments. These categories include NOFORN, ORCON, PROPIN, and SIOP. . Additionally, since the estimate was provided, SCI subcompartment identification and separation has become a significant issue in the SCI environment. There are approximately an order of magnitude more subcompartments than compartments. For these reasons, the estimate of originally provided (29) is too small and should be revised upward to a new initial point on an open scale.

page 84, Section 1.0.1.2, Testing

Change: Delete the last two sentences which specify the duration of the testing.

Rationale:
It is inappropriate to predetermine the length of the test period. Duration cannot be equated with quality in security testing and should not be used as the metric for quality.

page 84, Section 1.0.2.2, Testing

Change: Delete the last two sentences which specify the duration of the testing.

Rationale:
It is inappropriate to predetermine the length of the test period. Duration cannot be equated with quality in security testing and should not be used as the metric for quality.

page 85, Section 1.0.3.2, Testing

Change: Delete the last two sentences which specify the duration of the testing.

Rationale:
It is inappropriate to predetermine the length of the test period. Duration cannot be equated with quality in security testing and should not be used as the metric for quality.

page 87, Appendix A, Commerical Product Evaluation Process, first paragraph, third sentence beginning: "The formal evaluation is aimed at . . ."

Change: Replace " . . . and is completely divorced from any consideration of overall system performance, potential applications, or particular processing environments."
with: " . . . and while it is divorced from overall system performance, potential applications, or particular processing environments, a separate report measuring performance and commenting on performance implications of potential applications and procesing environments shall be made as part of the formal evaluation."

Rationale:
The cost effectiveness of the systems listed in the product evaluation list must be assessable by DoD elements selecting systems. Performance is the single most important factor in determining cost effectiveness, and as such, must be part of the evaluation package. There are use and environmental trade-offs which can be made to reduce the "systems" life cycle costs of the evaluated products if such information is made available to the DoD elements selecting certified systems.

page 91

Change: insert new class
"Class (C3): Labeled Object Protection

Class (C3) systems require all of the features of Class (C2). In addition, the capability must exist for accurate labeling of data to at least the granularity of a file and for labeling of exported information. The capability to audit changes in data labels must be present. Configuration management controls are required to manage source and object code changes. Device labels (for at least remote terminals) shall be present."

Rationale:
DCID minimum requirements for System High mode of operation differ from and are not compatible with class C2 nor B1 but rather fall between them, the requirements are:

- Remote terminal authentication
- Security classification and handling caveats identified with information in the system
- Labeling of output
- Audit trails
- Configuration Management Controls

page 91, Class (B1); Labeled Security Protection

Change: Replace paragraph
with: "Class (B1) systems require all the features for class (C3). In addition, an informal statement of the security policy model, and mandatory access control over named subjects and objects must be present. Any flaws identified by testing must be removed."

Rationale:
The reference to labeling has been removed as it is covered in the new class (C3).

page 94, Appendix D, Section: Audit

Change: Add the following paragraph
"C3: The TCB shall be able to audit any override of security label markings, and the use of user identification and authentication mechanisms."

Rationale:
To reflect the addition of Class C3.

page 94, Appendix D, Section: Configuration Management

Change: Add the following paragraph
"C3: A configuration management system shall be in place that maintains control of changes of any line of source or object code and records by whom, for what reason, and when the change is made. This system shall maintain up to date documentation of TCB design."

Rationale:
To reflect the addition of Class C3.

page 96, Section: Design Specification and Verification

Change: Replace phrase, beginning after B2, "A formal model of the security policy . . ."
with: "An informal or formal model of the security policy . . ."

Rationale:

An inconsistancy exists between requiring the formal model and permitting a Descriptive Top Level Specification (DTLS).

page 97, Section: Device Labels

Change: Add the following paragraph
"C3: The TCB shall support assignment of security levels to all remote physical devices, individually or in groups. These security levels shall be used by the TCB to enforce constraints imposed by the physical environment in which the devices are located."

Rationale:
To reflect the addition of Class C3.

page 97, Section: Discretionary Access Control

Change: Revise second sentence of C1 to read.
"The enforcement mechanism . . . shall allow users to specify and control sharing of those objects, initially generated by the user, by named individuals . . . ."

Rationale:
A user should only be capable of expanding access to objects which belong to the particular user, not for objects to which that user only has access. Otherwise any user could usurp the authority of the Data Base Administrator or System Security Officer.

page 97, Section: Discretionary Access Control

Change: Revise first sentence of C2 to read.
"The enforcement mechanism . . . shall allow users to specify and control sharing of those objects, initially generated by the user, by named individuals . . . ."

Rationale:
A user should only be capable of expanding access to objects which belong to the particular user, not for objects to which that user only has access. Otherwise any user could usurp the authority of the Data Base Administrator or System Security Officer.

page 97, Section: Discretionary Access Control

Change: Change sentence 4 of C2 to read
"Access permission to an object by users not already possessing access permission shall only be assigned by the user who initially generated the object and is still responsible and authorized to grant access or by the Data Base Administrator or System Security Officer for all other objects in the system."

Rationale:

A user should only be capable of expanding access to objects which belong to the particular user, not for objects to which that user only has access. Otherwise any user could usurp the authority of the Data Base Administrator or System Security Officer.

page 97, Section: Exportation of Labeled Information

Change: Add the following paragraph
"C3: The TCB shall be capable of associating a sensitivity label with all exported data."

Rationale:
To reflect the addition of Class C3.

page 98, Section: Exportation of Multilevel Devices

Change: Add the following paragraph
"C3: The TCB shall be capable of associating a sensitivity label with all exported data."

Rationale:
To reflect the addition of Class C3.

page 98, Section: Exportation of Single Level Devices

Change: Add the following paragraph
"C3: The TCB shall be capable of associating a sensitivity label with all exported data."

Rationale:
To reflect the addition of Class C3.

page 99, Section: Label Integrity

Change: Add the following paragraph
"C3: Sensitivity labels shall represent the security levels of objects with which they are associated. When exported by the TCB, sensitivity labels shall be associated with the information being exported."

Rationale:
To reflect the addition of Class C3.

page 99, Section: Labeling Human-Readable Output

Change: Add the following paragraph
"C3: Sensitivity labels shall be associated with human readable output."

Rationale:
To reflect the addition of Class C3.

page 100, Section: Labels

Change: Add the following paragraph
"C3: Sensitivity labels associated with each storage object which requires protection shall be maintained by the TCB. These labels shall support data marking on transmission to computers, nodes and terminals. Normally the security level of an object must be maintained throughout the life of the object. Changes to security levels must be mediated by the TCB or a trusted process which is invoked by a user who has special authority to change the security levels of objects."

Rationale:
To reflect the addition of Class C3.

page 101, Appendix D, Section: Object Reuse

Change: Add the following paragraph
"C1: The TCB shall be capable of clearing or overwriting any storage object."

Rationale:
To reflect DCI policy on object reuse.

page 103, Appendix D, Section: Trusted Distribution

Change: Add the following paragraph
"C3: A trusted ADP system control and distribution facility shall be provided for maintaining the integrity of the mapping between the master data describing the current version of the TCB and the on-site master copy of the code for the current version. Procedures shall exist for ensuring that the TCB software, firmware, and hardware updates distributed to a customer are exactly as specified by the master copies."

Rationale:
To reflect the addition of Class C3.

page 104, Appendix D, Section: Trusted Facility Management

Change: Add the following paragraph
"C3: The TCB shall support separate operator and administrator functions. The functions performed in the role of a security administrator shall be identified. The ADP system administrative personnel shall only perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the ADP system. Non-security functions that can be performed in the security administration role shall be limited to strictly to those essential to performing the security role effectively."

Rationale:
To reflect the addition of Class C3.

page 105, Appendix D, new Section titled "Formal Analysis" to be added after last entry on page.

Change: Add the following
"C3 - A1: Formal methods shall be used to investigate and document the behavior of the TCB under anomalous environmental conditions such as hardware failure."

Rationale:
Formal Design Verification Methods assume that the system being verified is closed and unaffected by environmental conditions. This is a reasonable assumption to make in verifying a design, but it should be extended with the notion that the real system will be open to influence from the environment. Formal methods can be used to investigate the behavior of a design under environmental influence (to a point). This additional step in use of formal verification technology should be incorporated into the criteria.

An instance of the specific use of such a methodology is due to L. J. La Padula, to be documented in part II, Vol. 4 of MTR 8756, DODIIS Security Protection for Information Exchange: Formal Design Verification of DNSIX.

page 105, Appendix D, new Section titled "Integrity/Deadlock Analysis" to be added after last entry on page.

Change: Add the following
"C1 - A1: Evidence shall be provided that deadlocks cannot occur or that they can be securely resolved by the TCB when they occur. Deadlock resolution algorithms shall be subjected to detailed analysis to provide such evidence. Evidence shall be provided that no critical datum is shared within the system that is controlled by the TCB. Scheduler algorithms and critical (unshareable) data allocation shall be subjected to detailed analysis to provide such evidence."

Rationale:
It has been shown that a system which employs an unrestricted, non-trivial scheduler has either a deadlock problem or a data integrity problem or both. The TCB would seem to employ such a scheduler as the mandatory security policy calls for dynamic realignment of resource allocations in consonance with changes in subject security level.

See 'Harmonious Cooperation of Processes Operating on a Common Set of Data,' parts 1,2, and 3, MTR-2254, 1972, D. E. Bell and L. J. La Padula.

page 105, Appendix D, new Section titled "Network Integrity/Stability" to be added after last entry on page.

Change: Add the following
"C1 - A1: An analysis shall be performed to show that the security provided by interacting TCBs is stable under the full range of normal networking operations, and the full range of possible TCB architectural combinations."

Rationale:
If an interaction is unstable, then it is difficult to see how it could be considered secure. Since interactions among non-symmetric TCBs will take place (such as the interconnection of a B2 and a C2 system), it is not clear that stability will be achieved. Therefore, it is not clear that security will be maintained.

page 111, in Glossary

Change: Add new definition as follows
"Low Water Mark - Of two or more security levels, the least of the hierarchical classifications, and the set intersection of the non-hierarchical categories."

Rationale:
Necessary to support the new definition of Session Security Level.

page 113, in Glossary

Change: Add new definition as follows
"Session Security Level - The security level of a session is the low water mark of the security levels of: the user, the terminal, a level specified by the user, and the system from which the session originates."

Rationale:
The session security level is a form of the user security level constrained by the level of the systems involved and possible voluntry restrictions imposed by the user. The session security level offers greater precision and protection than the user security level in an ADP environment in a form which permits you to transfer security relevant information both intra-and inter-host.

page 113, in Glossary, Simple Security Property definition

Change: replace
"A Bell-La Padula . . . security level of the subject dominates . . . ."
with: "A modified Bell-La Padula . . . security level of the session dominates . . . ."

Rationale:
Mandatory security enforcement should be based on the session security level not upon the subject (i.e. current user) security level. This protects against compromise which entities between the user and the object are not protected to levels as high as the user's security level. It also provides the opportunity for intelligence analysts on systems offering mandatory protection to voluntarily lower their session security level in order to extract information at lower than their user maximum classification level.

page 113, in Glossary, *Property definition

Change: replace with
"*-Property - A modified Bell-La Padula Model rule which precludes writing of information of a dominant security level into a container marked with a recessive security level and precludes writing above the session level. The *-Property prevents write down."

Rationale:
The *-property stated in this manner does not allow a write-up condition on the system. Such a write-up would allow a user to "bootstrap" his security level above that which the entire path is protected, and thus a violation of security policy. In Intelligence Community systems it would be rare and even dangerous to allow an unauthorized user to create a compartmented information file which might contain disinformation which would be acted upon by intelligence analysts. In the intelligence community both write up (receive only) and write down (downgrading, declassification, and sanitization) are currently handled by trusted processes especially designed and controlled for such operations.

page 113, in Glossary, Subject Security Level definition

Change: replace with
"Subject Security Level - A subject's security level is equal to the security level of the objects to which it has either read only or both read and write access. A subject's security level must always be dominated by the session security level."

Rationale:
This redefinition clarifies the least upper bound of the subject security level in cases where either, the user security level dominates the terminal security level, the user security level dominates the system security level, or the user desires to lower his maximum security level for a session.

page 115, References

Change: Add Reference to Defense Intelligence Agency Manual (DIAM) 50-4, "Security of Compartmented Computer Operations (U)," 24 June 1980 (CONFIDENTIAL)

Rationale:
DIAM 50-4 specifies the national level policy for foreign intelligence and Sensitive Compartmented Information (SCI) for DoD.

ANNEX 1

2.3 CLASS (C3): LABELED OBJECT PROTECTION

Class (C3) systems require all of the features of class (C2). In addition, the capability must exist for accurate labeling of data to at least the granularity of a file and for labeling of exported information. The capability to audit changes in data labels must be present. Configuration management controls are required to manage source and object code changes. The following are minimal requirements for systems assigned a class (C3) rating.

2.3.1 Security Policy

2.3.1.1 Discretionary Access Control

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects, initially generated by the user, by named individuals, or defined groups of individuals, or by both. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by the user who initially generated the object and is still responsible and authorized to grant access or by the Data Base Administrator or System Security Officer for all other objects in the system.

2.3.1.2 Object Reuse

When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the object contains no data for which the subject is not authorized.

2.3.1.3 Labels

Sensitivity labels associated with each storage object which requires protection shall be maintained by the TCB. These labels shall support data marking on transmission to computers, nodes and terminals. Normally the security level of an object must be maintained throughout the life of the object. Changes to security levels must be mediated by the TCB or a trusted process which is invoked by a user who has special authority to change the security levels of objects.

2.3.1.3.1 Label Integrity

Sensitivity labels shall represent the security levels of objects with which they are associated. When exported by the TCB, sensitivity labels shall be associated with the information being exported.

2.3.1.3.2 Exportation of Labeled Information

The TCB shall be capable of associating a sensitivity label with all exported data.

2.3.1.3.2.1 Exportation of Multilevel Devices

The TCB shall be capable of associating a sensitivity label with all exported data.

2.3.1.3.2.2 Exportation to Single-Level Devices

The TCB shall be capable of associating a sensitivity label with all exported data.

2.3.1.3.2.3 Labeling Human-Readable Output

Sensitivity labels shall be associated with human readable output.

2.3.1.3.3 Device Labels

The TCB shall support assignment of security levels to all remote physical devices, individually or in groups. These security levels shall be used by the TCB to enforce constraints imposed by the physical environment in which the devices are located.

2.3.2 Accountability

2.3.2.1 Identification and Authentication

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that is cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

2.3.2.2 Audit

The TCB shall be able to create, maintain and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user;s address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the action of any one or more users based on individual identity. **The TCB shall be able to audit any override of security label markings, and the use of user identification and authentication mechanisms.**

2.3.3 Assurance

2.3.3.1 Operational Assurance

2.3.3.1.1 System Architecture

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subject and objects in the ADP system. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

2.3.3.1.2 System Integrity

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

2.3.3.1.3 Trusted Facility Management

The TCB shall support separate operator and administrator functions. The functions performed in the role of a security administrator shall be identified. The ADP system administrative personnel shall only perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the ADP system. Non-security functions that can be performed in the security administration role shall be limited to strictly to those essential to performing the security role effectively.

2.3.3.1.4 Formal Analysis

Formal methods shall be used to investigate and document the behavior of the TCB under anomalous environmental conditions such as hardware failure.

2.3.3.1.5 Integrity/Deadlock Analysis

Evidence shall be provided that deadlocks cannot occur or that they can be securely resolved by the TCB when they occur. Deadlock resolution algorithms shall be subjected to detailed analysis to provide such evidence. Evidence shall be provided that no critical datum is shared within the system that is controlled by the TCB. Scheduler algorithms and critical (unshareable) data allocation shall be subjected to detailed analysis to provide such evidence.

2.3.3.1.6 Network Integrity/Stability

An analysis shall be performed to show that the security provided by interacting TCBs is stable under the full range of normal networking operations, and the full range of possible TCB architectural combinations.

2.3.3.2 Life-Cycle Assurance

2.3.3.2.1 Security Testing

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data. (See the Security Testing guidelines.)

2.3.3.2.2 Configuration Management

A configuration management system shall be in place that maintains control of changes of any line of source or object code and records by whom, for what reason, and when the change is made. This system shall maintain up to date documentation of TCB design.

2.3.3.2.3 Trusted Distribution

A trusted ADP system control and distribution facility shall be provided for maintaining the integrity of the mapping between the master data describing the current version of the TCB and the on-site master copy of the code for the current version. Procedures shall exist for ensuring that the TCB software, firmware, and hardware updates distributed to a customer are exactly as specified by the master copies.

2.3.4 Documentation

2.3.4.1 Security Features User's Guide

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

2.3.4.2 Trusted Facility Manual

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.

2.3.4.3 Test Documentation

The system developer shall provide to the evaluators a document that describes the test plan and results of the security mechanisms' functional testing.

2.3.4.4 Design Documentation

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.